## Frontline Defenders and Tactical Technology Collective (TTC),

## *Security-in-a-box*

The TTC toolkits provides sections on “how to protect yourself and your data when using social networking sites” and one called “how to use mobile phones as securely as possible.” These could be adapted and used to train humanitarian and development project teams, participants, and their mentors on safe and secure use of mobiles and social media sites. The safe social network use guide encourages thinking around who can access and use data and information, aspects of trust, safe use of passwords and privacy settings, browsing histories and secure access to the Internet. It also encourages analysis of friends, followers and contacts, status updates, location information, instant chats, and risks that may be present when joining or creating groups, events and communities. The chapter on mobile phone security explains security holes that are present in the use of mobile phones (commercial access to information, operating system security vulnerabilities, applications and vulnerability to interception). It also covers information vulnerabilities when communicating with others, and risks of geolocation, SMS interception, malware, SIM cards, and risks when connecting a phone to a laptop or computer.

## Digital Safe Spaces

Practitioners who work to create offline safe spaces for project participants, or ICTs end-users have identified a number of good practices. These can be adapted and replicated when creating safe online spaces for social, political and economic participation. Digital safe spaces are described as:

* End-user specific places with defined network ownership; trusted role models and mentors; opportunities for friendship and connection; with community buy-in and champions
* Spaces that protect end-users emotional well-being; where end-users can express themselves without judgment, take the lead to create fun, achieve common goals together; build trust in one another, and create ground rules that can be revisited and adapted over time
* Spaces that ensure end-users physical safety by achieving community buy-in for their safe participation; where end-users are free from harassment and can come and go safely; where new skills and ideas are carefully introduced in ways that do not put end-users at greater risk
* Spaces that are supported and curated by trusted mentors and role models who encourage end-users, convene and organize; share and engage end-users in new curricula and information; listen and play games; evaluate and ensure positive impact
* Spaces that involve end-users in identifying what, when and where they can be safe and support the creation of safety plans

## Children’s Online Privacy and Protection Act (COPPA)

As a US-based organization, NF will need to be aware of COPPA, the Children’s Online Privacy and Protection Act, enacted by the US Congress in 1998 to regulate the collection of personal information from children under 13 by persons or entities under US jurisdiction. COPPA applies only to companies operating websites directed at children under age thirteen or those operating general-audience websites that have “actual knowledge” that they are collecting personal information from children under thirteen. COPPA considers first and last name, address, e-mail address, telephone number, Social Security Number, any other identifier that the FTC determines that permits the physical or online contacting of a specific individual as “personally identifying information.” COPPA has been criticized for not requiring websites to enforce age verification of visitors, which makes enforcement difficult. It’s simple also for children under 13 to provide a false age. Companies operating websites that fall outside COPPA’s jurisdiction but that target young people are under the watch of the FTC, which can enforce commitments made to Internet users under privacy policies under the FTC’s general unfair and deceptive practices powers. The FTC considers the use or dissemination of personal information in a manner contrary to a posted privacy policy as a deceptive practice .

## Privacy Impact Assessments

“Privacy Impact Assessments” (PIA) are a tool to help designers analyze privacy risks and mitigate or manage them. A PIA is a structured assessment of how personal information is handled, and it addresses the legal, regulatory, policy and ethical requirements regarding privacy. It identifies the risks and effects of collecting, processing and disseminating information and demonstrates awareness of the context in which such information may be used. It analyzes and evaluates technical safeguards and protections for handling information to mitigate privacy risks. It also addresses unforeseen disclosure of datasets. In extreme contexts, the “do no harm” principle may need to be invoked. This principle is applicable in settings where the potential harm posed to individuals by data insecurity and personal identification is so high that it could lead to arrest, torture, death and/or longstanding discrimination. In this case, it is possible that data should not be collected at all given the high levels of risk not outweighing the benefits of the effort.

## Participatory Risk Analysis example: GSMA matrix

A risk assessment is a way of considering the balance of risks and benefits, based on reasonableness. There is not yet a widely used comprehensive and quantitative method to assess privacy risk, but as a humanitarian or development project moves into design and development, one should be developed that fits with the organizational context. The GSMA, for example, used the following matrix to work with students, teachers, parents and the wider education community to identify potential concerns and risks with mobile education: A similar matrix should be developed for GEM with input from key stakeholders in order to identify and put into place risk mitigation strategies that are relevant to the local context and that can be later consolidated and rolled into the global design of the platform.

# Additional Resources

|  |  |  |  |
| --- | --- | --- | --- |
| **Organization/Individual** | **Initiative(s)** | **Notes** | **More info:** |
| Internews  <https://www.internews.org> | Speak Safe | <https://internews.org/research-publications/speaksafe-media-workers-toolkit-safer-online-and-mobile-practices> Online version doesn’t work (have to download a pdf)  Oriented towards a single user protecting their privacy | Contact: Jon Camfield |
| Level up | <https://www.level-up.cc/> |
| Tactical Tech  <https://tacticaltech.org> | Security in a Box/ Security in Context | <https://securityinabox.org> |  |
| ICRC | Produced protection standards in 2013 | <https://www.icrc.org/eng/resources/documents/publication/p0999.htm> |  |
| New America Foundation / Open Technology Institute | [Dialing Down Risk: Mobile Privacy and Information Security for in Global Development](http://newamerica.net/publications/policy/dialing_down_risks_mobile_privacy_and_information_security_in_global_development) | <http://newamerica.net/publications/policy/dialing_down_risks_mobile_privacy_and_information_security_in_global_development> | Contact: Hibah Hussein |
| The [International Principles on the Application of Human Rights to Communications Surveillance](https://en.necessaryandproportionate.org/text) (“The Principles”). // maybe | 13 principles related to communications surveillance and human rights. (See annex) | <https://www.accessnow.org/blog/2013/07/31/over-100-global-civil-society-groups-release-human-rights-principles-to-gov?utm_content=buffer62e9c&utm_source=buffer&utm_medium=twitter&utm_campaign=Buffer> |  |
| WWW Foundation and  IDRC | Privacy in the Developing World Network  Open Data in Developing Countries network | <http://www.opendataimpacts.net/>  <http://www.opendataresearch.org/content/2013/501/open-data-privacy-discussion-notes>  <http://www.opendataresearch.org/project/2013/oddc> | Contact: Tim Davies |
| GSMA | Privacy by Design | <http://www.gsma.com/publicpolicy/privacy-design-guidelines-for-mobile-application-development> |  |
| The Engine Room | Social Tech Census / Index // this is a collection of (mostly) organizations | https://socialtechcensus.org/ |  |
| Video 4 Change // collection of videos/resources with a category on safety/security | Guidelines on use of video to document, incl human rights abuses | <https://www.v4c.org/category/safety-and-security>  https://www.v4c.org/content/conducting-safe-effective-and-ethical-interviews-survivors-sexual-and-gender-based-violence |  |
| Aiding Surveillance: An Exploration of How Development and Humanitarian Aid Initiatives are Enabling Surveillance in Developing Countries | Privacy International supported by ICRD | <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2326229> | Contact: Carly Nyst |
| NYU School of Law - Big Data and Privacy - reducing predictive harm | Paper | http://lsr.nellco.org/cgi/viewcontent.cgi?article=1434&context=nyu\_plltwp |  |
| Patrick Meier et al | Shared principles for big data and resilience | http://irevolution.net/2013/09/23/principles-for-big-data-and-resilience/ |  |
| Freedom House | Safety on the Line | <http://www.freedomhouse.org/sites/default/files/Safety%20on%20the%20Line.pdf> |  |
| [*New America Foundation Open Technology Institute*](http://oti.newamerica.net/)  [*University of Pennsylvania*](http://cgcs.asc.upenn.edu/cgi-bin/projects.cgi?id=105&p=main) *(*[*Global Engagement Fund*](http://global.upenn.edu/gef)*,* [*Center for Global Communications Studies*](http://cgcs.asc.upenn.edu/index.html) *at the Annenberg School and the* [*Zicklin Center for Business Ethics Research*](https://lgst.wharton.upenn.edu/research/research-centers/the-carol-and-lawrence-zicklin-center-for-business-ethics-research/) *at Wharton)*  [*Internews Center for Innovation and Learning*](http://www.internews.org/global-issues/center-innovation-and-learning)  [*Centre for Internet and Society*](http://cis-india.org/)*, Bangalore*  [*Center for Media and Communications Studies*](https://cmcs.ceu.hu/)*, Central European Univeristy, Budapest*  [*Alexander Von Humboldt Institute for Internet and Society*](http://www.hiig.de/en/)*, Berlin*  *Instituto de Tecnologia e Sociedade, Brazil*  [*Access*](https://www.accessnow.org/) | Ranking Digital Rights project | http://rankingdigitalrights.org/ |  |
| (from Bali Internet forum, 2013) | Big data and privacy | http://www.rappler.com/world/regions/asia-pacific/42116-big-data-philanthropy-privacy-invasion |  |
| Bellagio/PopTech | Big data and ethics and resilience | <http://poptech.org/system/uploaded_files/66/original/BellagioFramework.pdf> |  |
| Evgeny Morozov | Why privacy is a political problem | http://www.technologyreview.com/featuredstory/520426/the-real-privacy-problem/?src=longreads |  |
| Source - [Jonathan Stray](https://source.opennews.org/people/jonathan-stray/) | SECURITY FOR JOURNALISTS, PART TWO: THREAT MODELING | https://source.opennews.org/en-US/learning/security-journalists-part-two-threat-modeling/ |  |
| Privacy International // A lot of good stuff by them | Biometrics: Friend or Foe | http://pi.dev.uberdigital.com/resources/reports/biometrics-friend-or-foe-of-privacy |  |

Please also see additional resource mapping from The Engine Room: <https://docs.google.com/spreadsheet/ccc?key=0AstZ6Hn7MaXHdE5UWmlCdk1WczVQbWFRY3dlNzlrMFE&usp=gmail#gid=0>